SENATE BILL NO. _____ HOUSE BILL NO. _____

A BILL to amend the Code of Virginia by adding in Title 2.2 a Chapter 4.3, consisting of sections numbered 2.2-435.9 and 2.2-435.10, by adding in article 35 of Chapter 26 of Title 2.2 a sectioned numbered 2.2-2699.8 and by adding in Chapter 3 of Title 8.01 an article numbered 26, consisting of sections numbered 8.01-227.24 through 8.01-227.27, relating to electronic identity providers; liability.

Be it enacted by the General Assembly of Virginia:

1. That the Code of Virginia is amended by adding in Title 2.2 a Chapter 4.3, consisting of sections numbered 2.2-435.9 and 2.2-435.10, by adding in article 35 of Chapter 26 of Title 2.2 a sectioned numbered 2.2-2699.8 and by adding in Chapter 3 of Title 8.01 an article numbered 26, consisting of sections numbered 8.01-227.24 through 8.01-227.27, as follows:

CHAPTER 4.3

COMMONWEALTH IDENTITY MANAGEMENT STANDARDS

§ 2.2-435.9. Approval of Electronic Identity Standards.

The Secretary of Technology and the Secretary of Transportation shall review and approve or disprove, upon the recommendation of the Information Technology Advisory Council pursuant to § 2.2-2699.6, the adoption of (a) nationally recognized technical and data standards regarding the verification and authentication of identity in digital and online transactions, (b) the minimum specifications and standards that should be included in an identity trust framework so as to warrant liability protection pursuant to the Electronic Identity Liability Protection Act (§ 8.01-227.24 et seq.), and (c) any other related data standards or specifications concerning reliance by third parties on identity credentials.

§ 2.2-435.10. Publication of Standards

The Secretary of Technology and the Secretary of Transportation shall cause the standards and specifications adopted pursuant to this Chapter be published in multiple locations, including but not limited in the Virginia Administrative Code and on the website of the Secretary of Technology, the Secretary of Transportation, and the Virginia Economic Development Partnership, the minimum

specifications and standards that must be included in an identity trust framework so as to warrant liability protection pursuant to the Electronic Identity Liability Protection Act (§ 8.01-227.24 et seq.).

§ 2.2-2699.6. Powers and duties of the ITAC.

A. The ITAC shall have the power and duty to:

1. Adopt rules and procedures for the conduct of its business;

2. Advise the CIO on the development of all major information technology projects as defined in § 2.2-2006;

3. Advise the CIO on strategies, standards, and priorities for the use of information technology for state agencies in the executive branch of state government;

4. Advise the CIO on developing the two-year plan for information technology projects;

5. Advise the CIO on statewide technical and data standards for information technology and related systems, including the utilization of nationally recognized technical and data standards for health information technology systems or software purchased by a state agency of the Commonwealth;

6. Advise the CIO on statewide information technology architecture and related system standards;

7. Advise the CIO on assessing and meeting the Commonwealth's business needs through the application of information technology;

8. Advise the CIO on the prioritization, development, and implementation of enterprise-wide technology applications; annually review all agency technology applications budgets; and advise the CIO on infrastructure expenditures; ~~and~~

9. Advise the CIO on the development, implementation, and execution of a technology applications governance framework for executive branch agencies. Such framework shall establish the categories of use by which technology applications shall be classified, including but not limited to enterprise-wide, multiagency, or agency-specific. The framework shall also provide the policies and procedures for determining within each category of use (i) the ownership and sponsorship of applications, (ii) the proper development of technology applications, (iii) the schedule for maintenance or enhancement of applications, and (iv) the methodology for retirement or replacement of applications.

ITAC shall include the participation of agency leaders who are necessary for defining agency business needs, as well as agency information technology managers who are necessary for overseeing technology applications performance relative to agency business needs. Agency representatives shall assist ITAC in determining the potential information technology solutions that can meet agency business needs, as well as how those solutions may be funded; and

10. Advise the Secretary of Technology and the Secretary of Transportation, upon the recommendation of the Electronic Identity Standards Advisory Committee pursuant to § 2.2-2699.8, on the adoption of (a) nationally recognized technical and data standards regarding the verification and authentication of identity in digital and online transactions, (b) the minimum specifications and standards that should be included in an identity trust framework so as to warrant liability protection pursuant to the Electronic Identity Liability Protection Act (§ 8.01-227.24 et seq.), and (c) any other related data standards or specifications concerning reliance by third parties on identity credentials.

B. Definitions.

As used in this section, the term "technology applications" includes, but is not limited to, hardware, software, maintenance, facilities, contractor services, goods, and services that promote business functionality and facilitate the storage, flow, use or processing of information by agencies of the Commonwealth in the execution of their business activities.

§ 2.2-2699.8. Electronic Identity Standards Advisory Committee.

A. The ITAC shall appoint an advisory committee of persons with expertise in electronic identity management and information technology to advise the ITAC on (i) the utilization of nationally recognized technical and data standards regarding the verification and authentication of identity in digital and online transactions, (ii) the minimum specifications and standards that should be included in an identity trust framework so as to warrant liability protection pursuant to the Electronic Identity Liability Protection Act (§ 8.01-227.24 et seq.), and (iii) the use or adoption of any other related data standards or specifications concerning reliance by third parties on identity credentials.

B. The advisory committee shall consist of seven members. Members shall be appointed based upon recommendations of the Secretary of Technology and the Secretary of Transportation, and shall

include a representative of the Department of Motor Vehicles, the Virginia Information Technology Agency, and representatives of the business community with appropriate experience and expertise. Members appointed to serve on the advisory committee shall serve without compensation, but shall be reimbursed for all reasonable and necessary expenses incurred in the performance of their duties as provided in § 2.2-2825. In addition to the appointed members, the CIO, the Secretary of Technology, and the Secretary of Transportation, or their designees, may also serve on the advisory committee.

C. The advisory committee shall collaborate with relevant state agencies and private sector entities as necessary and appropriate to develop its recommendations.

D. Terms used in this section shall have the same meaning as set forth in § 8.01-227.24.

Article 26.

~~Identity Management Liability.~~Electronic Identity Liability Protection Act

§ 8.01-227.24. Definitions.

As used in this article unless the context requires a different meaning:

"Commonwealth identity management standards" means the standards and specifications approved by the Secretary of Technology and the Secretary of Transportation pursuant to Chapter 4.3 (§ 2.2-435.9 et seq.) of Title 2.2 that establish the minimum specifications and standards that must be included in an identity trust framework so as to warrant liability protection pursuant to this article.

~~"Federated identity management" means a digital identity system that allows individuals, previously issued an identity credential, to use the same identity data (which, by way of example and not limitation, may be stored on an identity credential or identity token) to access resources (networks, databases, facilities, or other similar assets) of more than one enterprise within an identity trust framework in order to aid access control, conduct transactions and share information.~~

"Identity attribute" means ~~personal~~ identifying information associated with an identity credential holder.

"Identity credential" means the ~~identity~~ data ~~or the container for identity data which forms a~~, or the physical object upon which the data resides, that an identity credential holder may present to verify or authenticate his identity in a digital or online transaction ~~verifiable assertion of identity when~~

~~presented in an authentication transaction. The identity credential can be bound in some way to the identity credential holder to whom or to what it was issued, or it can be unbound, as with a bearer credential~~.

"Identity credential holder" is a person bound to or ~~is~~ in possession of an identity credential ~~and~~ who has agreed to ~~be bound by~~ the terms and conditions ~~required by~~ of the identity provider.

"Identity proofer" means ~~an individual~~ a person or entity authorized to act as a representative of an identity provider in the confirmation of a potential identity credential holder's identification and identity attributes ~~during the registration process~~ prior to issuing an identity credential to a person. ~~An identity proofer may also be known as a registration authority, local registration agent, trusted agent, or notary acting to verify the individual's identity.~~

"Identity provider" means ~~a certified~~ an entity, or a supplier, employee, or agent thereof, ~~within~~ certified by an identity trust framework ~~responsible for providing the~~ to provide identity ~~credential~~ credentials that may be used by an identity credential holder to assert his identity, in a digital or online environment. For purposes of this article, "identity provider" shall also include an attribute provider, an identity proofer, and any suppliers, employees, or agents thereof ~~and/or asserting an identity and/or identity attribute for that identity credential holder~~.

~~"Identity token" means hardware the identity credential holder possesses that contains the identity credential.~~

"Identity trust framework" ~~in~~ means a digital identity ~~systems~~ system ~~is a certification program that enables the relying party to trust the~~ with established identity, security, and privacy rules and policies ~~of the party who issues the identity credential~~ adhered to by certified identity providers that are members of the identity trust framework. ~~Participants~~ Members of an identity trust framework include identity trust framework ~~providers,~~ operators and identity providers~~, identity attribute providers, identity credential holders, and relying~~. Relying parties may, but are not required, to be a member of an identity trust framework in order to accept an identity credential issued by a certified identity provider to verify an identity credential holder's identity.

"Identity trust framework ~~provider~~ operator" means ~~an~~ the entity that ~~may~~ (a) ~~define~~ defines rules and policies for member parties to ~~its~~ a respective trust framework, (b) certifies identity providers to be members of and issue identity credentials pursuant to the trust framework, ~~;evaluate~~and (c) evaluates participation in the trust framework to ensure compliance by members of the identity trust framework with ~~policy~~ its rules and policies, including the ability to request audits of participants for verification of ~~such~~ compliance; and certifies identity providers to issue identity credentials pursuant to the trust framework~~., and/or (c) bestow one or more trustmarks on identity providers within the trust framework~~.

"Relying party" is an individual or entity that relies on the validity of an identity credential or an associated trustmark.

"Trustmark" means a machine-readable official seal, authentication feature, certification, license, or logo that may be provided by a trust framework operator to certified identity providers within its identity trust framework ~~that signifies~~ to signify that the identity provider complies with ~~identity trust framework compliance with~~ the ~~system~~ trust framework rules and policies ~~of the applicable identity trust framework as determined by its accreditation or certification authority.~~

§ 8.01-227.25. Trustmark ~~does not carry implied warranty;~~ warranty.

~~The use of a trustmark in a transaction does not imply a warranty for accuracy of the underlying informational content involved in the transaction. Nothing in this article shall prevent an identity provider from providing a warranty for the assertion of identity contained on the identity credential.~~

A. The use of a trustmark on an electronic identity credential provides a warranty solely for the assertion of the identity and any attributes of the identity credential holder contained on the identity credential, but does not create an implied warranty for any other element of the specific transaction for which the identity is asserted.

§8.01-227.26. ~~Liability and~~ Civil immunity.

A. ~~An~~ No identity trust framework ~~provider~~ operator shall be ~~immune from suit arising from~~ liable for civil damages arising from any acts or omissions relating to (i) the ~~provisioning an identity attribute,~~ issuance of an identity credential or assignment of an identity attribute to an identity credential holder~~, identity token, or trustmark issued in accordance with the specifications of identity trust~~

~~frameworks, including systems supporting federated identity management, that the Commissioner of the Department of Motor Vehicles for the Commonwealth of Virginia has deemed acceptable, unless the identity trust framework provider was grossly negligent or engaged in willful misconduct~~ or (ii) the issuance of a trustmark to a identity provider, provided that the credential, attribute, or trustmark was issued in accordance with the specifications of the operator's identity trust framework that meets or exceeds the Commonwealth's identity management standards.

B. ~~An~~ No identity provider shall be ~~immune from suit arising from~~ liable for civil damages arising from any acts or omissions relating to ~~identity proofer actions, provisioning~~ the issuance of an ~~identity attribute,~~ identity credential or assignment of an attribute to an identity credential holder, ~~or identity token issued in accordance with the specifications of identity trust frameworks that the Commissioner of the Department of Motor Vehicles for the Commonwealth of Virginia has deemed acceptable, unless the identity provider was grossly negligent or engaged in willful misconduct~~ provided that the credential or attribute was issued or assigend in accordance with the specifications of the trust framework of which the provider is a member that meets or exceeds the Commonwealth's identity management standards.

C. Nothing in subsection A or B shall prevent or limit the liability of an identity trust framework operator or an identity provider if the operator or provider commits and act or omission that (i) constitutes gross negligence or willful misconduct, or (ii) does not adhere to the rules and policies of its respective trust framework that meets or exceeds Commonwealth identity management standards.

§ 8.01-227.27. Sovereign Immunity.

No provisions of this article nor any act or omission of a state, regional, or local governmental entity related to the issuance of electronic identity credentials or attributes or the administration or participation in an identity trust framework related to the issuance of electronic identity credentials or attributes shall be deemed a waiver of sovereign immunity to which the governmental entity or its officers, employees, or agents are otherwise entitled.

#